IB03/04121

PCT/IB03/04121

19.09.03

SCHWEIZERISCHE EIDGENOSSENSCHAFT
CONFÉDÉRATION SUISSE
CONFEDERAZIONE SVIZZERA

Rec'd PCT/PTO 23 MAR 2005



10/528788

**Bescheinigung**

Die beiliegenden Akten stimmen mit den ursprünglichen technischen Unterlagen des auf der nächsten Seite bezeichneten Patentgesuches für die Schweiz und Liechtenstein überein. Die Schweiz und das Fürstentum Liechtenstein bilden ein einheitliches Schutzgebiet. Der Schutz kann deshalb nur für beide Länder gemeinsam beantragt werden.

**Attestation**

Les documents ci-joints sont conformes aux pièces techniques originales de la demande de brevet pour la Suisse et le Liechtenstein spécifiée à la page suivante. La Suisse et la Principauté de Liechtenstein constituent un territoire unitaire de protection. La protection ne peut donc être revendiquée que pour l'ensemble des deux Etats.

**Attestazione**

I documenti allegati sono conformi agli atti tecnici originali della domanda di brevetto per la Svizzera e il Liechtenstein specificata nella pagina seguente. La Svizzera e il Principato di Liechtenstein formano un unico territorio di protezione. La protezione può dunque essere rivendicata solamente per l'insieme dei due Stati.

Bern, 11. SEP. 2003

Eidgenössisches Institut für Geistiges Eigentum
Institut Fédéral de la Propriété Intellectuelle
Istituto Federale della Proprietà Intellettuale

Patentverfahren
Administration des brevets
Amministrazione dei brevetti

H. Jenni

Heinz Jenni

Demande de brevet no 2002 1623/02

CERTIFICAT DE DEPOT (art. 46 al. 5 OBI)

L'Institut Fédéral de la Propriété Intellectuelle accuse réception de la demande de brevet Suisse dont le détail figure ci-dessous.

Titre:
Système de déchiffrement de données à accès contitionnel.

Requérant:
Nagravision S.A.
22, Route de Genève
1033 Cheseaux-sur-Lausanne

Mandataire:
Leman Consulting S.A.
62 rte de Clementy
1260 Nyon

Date du dépôt: 27.09.2002

Classement provisoire: G06F

# Système de déchiffrement de données à accès conditionnel

La présente invention concerne un système de déchiffrement de données à accès conditionnel.

De tels systèmes sont notamment utilisés dans le domaine de la télévision numérique à péage. Dans ce cas, le flux numérique de données transmis vers le téléviseur est chiffré afin de pouvoir en contrôler l'utilisation et de définir des conditions pour une telle utilisation. Ce chiffrement est réalisé grâce à des mots de contrôle (Control Words) qui sont changés à intervalle régulier (typiquement entre 5 et 30 secondes, bien que des intervalles nettement plus longs puissent être utilisés) afin de dissuader toute attaque visant à retrouver un tel mot de contrôle.

Pour que le récepteur puisse déchiffrer le flux chiffré par ces mots de contrôle, ces derniers lui sont envoyés indépendamment du flux dans des messages de contrôle (ECM) chiffrés par une clé propre au système de transmission entre un centre de gestion et un module de sécurité de l'unité d'utilisateur. En effet, les opérations de sécurité sont effectuées dans un module de sécurité (SC) qui est généralement réalisé sous la forme d'une carte à puce, réputée inviolable. Ce module peut être soit de type amovible soit directement intégrée au récepteur.

Lors du déchiffrement d'un message de contrôle (ECM), il est vérifié, dans le module de sécurité (SC), que le droit pour accéder au flux considéré est présent. Ce droit peut être géré par des messages d'autorisation (EMM) qui chargent un tel droit dans le module de sécurité. D'autres possibilités sont également envisageables telles que l'envoi de clés de déchiffrement.

Pour la suite de l'exposé, on appellera "événement" un contenu vidéo, audio (par exemple MP3) ou données (programme de jeu par exemple) qui est chiffré selon la méthode connue des mots de contrôle, chaque événement pouvant être chiffré par un ou plusieurs mots de contrôle, chacun ayant une durée de validité déterminée.

La comptabilisation de l'utilisation de tels événements est aujourd'hui basée sur le principe de l'abonnement, de l'achat d'événements ou du paiement par unité de temps.

L'abonnement permet de définir un droit associé à un ou des canaux de diffusion transmettant ces événements et permet à l'utilisateur d'obtenir ces canaux en clair si le droit est présent dans son module de sécurité.

Parallèlement, il est possible de définir des droits propres à un événement, tel qu'un film ou un match de football. L'utilisateur peut acquérir ce droit (achat par exemple) et cet événement sera spécifiquement géré par ce droit. Cette méthode est connue sous l'appellation "pay-per-view" (PPV).

Pour ce qui concerne le paiement par unité de temps, le module de sécurité comprend un crédit qui est débité en fonction de la consommation réelle de l'utilisateur. Ainsi par exemple, une unité sera débitée chaque minute à ce crédit quel que soit le canal ou l'événement regardé. Il est possible selon les implémentations techniques, de varier l'unité de comptabilisation, soit dans la durée, soit dans la valeur du temps alloué, voire en combinant ces deux paramètres pour adapter la facturation au type d'événement transmis.

Un message de contrôle (ECM) ne contient pas uniquement le mot de contrôle, mais également les conditions pour que ce mot soit renvoyé au récepteur/décodeur. Lors du déchiffrement des mots de contrôle, il sera vérifié si un droit associé aux conditions d'accès énoncées dans le message est présent dans le module de sécurité.

Le mot de contrôle n'est retourné à l'unité d'utilisateur que lorsque la comparaison est positive. Ce mot de contrôle est contenu dans un message de contrôle ECM qui est chiffré par une clé de transmission.

Pour que le droit soit présent dans le module de sécurité, il est généralement chargé dans ce module par un message d'autorisation (EMM) qui pour des raisons de sécurité, est généralement chiffré par une clé différente dite clé de droit (RK).

Selon une forme connue de diffusion de télévision à péage, les trois éléments suivants sont nécessaires pour déchiffrer un événement à un moment donné:

- les données relatives à l'événement chiffré par un ou une pluralité de mots de contrôle (CW),

- le ou les messages de contrôle ECM contenant les mots de contrôle (CW) et les conditions d'accès (AC)

- le droit correspondant stocké dans le module de sécurité permettant de vérifier les dites conditions d'accès.

Les systèmes de déchiffrement du type décrit ci-dessus sont actuellement tous formés d'équipements relativement grands. Ils sont reliés à un dispositif d'exploitation ou de visualisation tel que par exemple une télévision au moyen d'un câble. Ils ne sont pas prévus pour pouvoir être déplacés facilement. Il n'est donc pas possible de déplacer son propre décodeur et de le raccorder simplement sur une autre télévision, et d'acquérir des droits ponctuels. De plus, dans les systèmes actuels, relativement peu d'installations ont une ligne de retour permettant de communiquer depuis le décodeur vers un centre de gestion. Les installations qui ont une ligne de retour n'ont pas d'interface permettant de communiquer de façon conviviale avec ce centre de gestion. En effet, les lignes de retour sont prévues pour une communication entre le décodeur et le centre de gestion, mais pas entre l'utilisateur et ce centre. Il est ainsi malaisé d'acquérir des droits ponctuels de façon rapide et simple. De plus, dans tous les systèmes connus, les flux contenant les données, les messages de contrôle et les messages d'autorisation proviennent d'une source unique qui gère ses propres abonnements, sans pouvoir offrir une gamme d'abonnements de différentes sources.

La présente invention se propose de pallier les inconvénients des systèmes de l'art antérieur et de réaliser un système qui puisse facilement être déplacé et utilisé sur pratiquement n'importe quel dispositif d'exploitation adapté. De plus, un tel système simplifie la gestion des droits d'accès au niveau du centre de diffusion et offre une plus grande souplesse à l'utilisateur.

Ces buts sont atteints par un système tel que défini en préambule et caractérisé en ce qu'il comporte

- un premier centre de diffusion agencé pour diffuser des données chiffrées par des mots de contrôle (cw), ces mots de contrôle étant transmis dans des messages de contrôle (ECM) par ce premier centre de diffusion,

- au moins un deuxième centre de diffusion agencé pour diffuser des messages d'autorisation (EMM) relatifs aux droits d'accès aux données chiffrées et pour gérer ces droits d'accès,
- un dispositif d'exploitation destiné à rendre utilisables lesdites données chiffrées, et
- un décodeur agencé pour déchiffrer au moins une partie des données chiffrées, interposé entre le premier centre de diffusion et le dispositif d'exploitation,

en ce que le décodeur est formé d'un module de réception des données chiffrées et d'un module de gestion des droits d'accès à ces données, le module de réception étant connecté au dispositif d'exploitation et le module de gestion étant agencé pour communiquer avec le module de réception,

en ce que le module de gestion comporte un module de sécurité agencé pour vérifier le contenu des messages d'autorisation et pour permettre ou empêcher le déchiffrement des mots de contrôle et des données chiffrées en fonction du contenu des messages d'autorisation,

et en ce que le module de réception reçoit les données chiffrées provenant du premier centre de diffusion ainsi que les mots de contrôle, et le module de gestion reçoit les messages d'autorisation (EMM) du deuxième centre de diffusion.

La présente invention et ses avantages seront mieux compris en référence à la description de différents modes de réalisation et aux dessins annexés, dans lesquels :

- la figure 1 représente une vue d'ensemble d'un premier mode de réalisation du système selon la présente invention; et
- la figure 2 est une vue d'ensemble d'un deuxième mode de réalisation de l'invention.

En référence à ces figures, le système de l'invention comporte essentiellement un premier centre de diffusion 10 agencé pour diffuser des données chiffrées, au moins un deuxième centre de diffusion 11 agencé pour diffuser des messages

d'autorisation (EMM) et traiter la gestion de droits d'accès aux données chiffrées, un dispositif d'exploitation 12 destiné à rendre utilisables, ces données chiffrées et un décodeur 13 agencé pour déchiffrer au moins une partie des données chiffrées.

Le premier centre 10 de diffusion de données chiffrées peut être un dispositif classique par câble ou par satellite notamment. Ce centre émet des données sous forme chiffrées. La nature de ces données dépend bien entendu de l'utilisation qui doit en être faite. Dans la suite du texte, il est supposé que les données sont utilisées dans un système de télévision à accès conditionnel. Les données sont donc formées d'un contenu vidéo CT, c'est-à-dire des images et du son. D'autres données spécifiques à l'utilisation peuvent également être inclues, de façon bien connue de l'homme du métier. Ces données, ou au moins une partie d'entre elles, sont chiffrées au moyen de mots de contrôle et sont notées cw(CT) sur les figures.

Les mots de contrôle cw sont transmis, sous forme chiffrée, par le premier centre de diffusion en même temps que les données chiffrées.

Le, ou plus généralement les deuxièmes centres 11 de diffusion sont chargés de gérer les droits d'accès aux données. Ils peuvent chacun gérer des types de droits différents, notamment des abonnements, des accès ponctuels, des bouquets de programmes différents. Pour réaliser ceci, ils diffusent également les messages d'autorisation (EMM) correspondants, à destination des décodeurs concernés.

Le dispositif d'utilisation 12 est également bien entendu adapté aux données à transmettre. Dans le cas choisi de la télévision à accès conditionnel, le dispositif d'exploitation est un téléviseur.

Le décodeur 13 comporte un module de réception 14 des données et un module de gestion 15 des droits d'accès à ces données. Le module de gestion des droits est réalisé de telle façon qu'il soit aisément portable. Il peut judicieusement être réalisé au moyen d'un téléphone portable. Le module de gestion comporte également un module de sécurité 16. Dans le cas où des opérateurs différents ne souhaitent pas intégrer leur sécurité sur un module commun, ou simplement pour augmenter la souplesse d'utilisation, il est possible de prévoir une connectique

permettant soit de changer facilement de module de sécurité, soit d'en utiliser plusieurs à la fois. Ces modules peuvent être réalisés sous la forme d'une carte à puce coopérant avec un lecteur approprié du module de gestion, ou sous une forme plus compacte permettant la mise en place de plusieurs modules de sécurité simultanément. Dans ce cas, chaque puce gère les autorisations provenant de l'un des deuxièmes centres de diffusion.

Il est également possible de prévoir une carte ou un autre support comportant plusieurs puces, chacune d'elles gérant les autorisations provenant de l'un des deuxièmes centres de diffusion. Un tel module de sécurité est illustré par la figure 2, sous la référence 16.

Le module de gestion 15 comporte avantageusement un lecteur de carte à puce destiné à être utilisé avec une carte de crédit ou une carte à prépaiement 17. De cette façon, la gestion des paiements est assurée lorsqu'un évènement est commandé. Ceci permet en outre d'utiliser le module de gestion comme porte-monnaie électronique. Une telle carte est illustrée sous la référence 17 dans la figure 2.

Le module de réception 14 des données peut être intégré directement dans l'appareil de télévision 12. Dans ce cas, pour pouvoir lire des données chiffrées sur un tel téléviseur, il suffit de disposer du module de gestion 15 et des droits correspondants à l'événement souhaité. Cet événement peut donc être visualisé à partir de n'importe quel téléviseur équipé de façon adéquate. Ce mode de réalisation est illustré schématiquement par la figure 2. Selon une autre forme de réalisation avantageuse, il peut être formé d'un boîtier qui peut être connecté à la télévision au moyen d'un câble de connexion ou directement par une sortie sur la télévision. Ceci permet d'utiliser de façon simple, la présente invention sur des téléviseurs existants.

Le système selon l'invention fonctionne de la manière suivante :

Comme mentionné précédemment, le contenu vidéo CT est diffusé par le premier centre de diffusion 10 de données chiffrées. Simultanément, ce premier centre diffuse également les mots de contrôle cw qui ont été utilisés pour chiffrer les données. Lorsque l'on souhaite utiliser des données du système à accès conditionnel, par exemple, pour voir un événement tel qu'un film ou un match de

football par exemple, pour lequel l'accès est soumis à un droit, il est tout d'abord nécessaire d'acquérir ce droit. Celui-ci peut être donné par une carte à pré-paiement disposée dans le module de gestion 15, ou il peut être chargé dans ce module grâce aux moyens de communication entre le module et l'un des deuxièmes centres 11 de diffusion, qui gère les droits d'accès.

Pour obtenir les messages d'autorisation EMM qui vont permettre le déchiffrement des mots de contrôle cw nécessaire au déchiffrement des données et donc à la visualisation de l'évènement, le module de réception 13 établi une communication avec l'un des deuxièmes centres de diffusion. Comme mentionné précédemment, le module de réception peut être formé d'un téléphone portable. Dans ce cas, le contact est établi en composant un numéro de téléphone correspondant au centre de diffusion. Le choix de l'événement pour lequel on souhaite acquérir les droits se fait au moyen d'un "menu" préenregistré, chaque choix du menu correspondant à un numéro particulier sur le clavier du téléphone portable. Le téléchargement du message d'autorisation correspondant à l'évènement choisi se fait après avoir pressé une touche de validation sur le clavier du téléphone.

Le module de déchiffrement 14 est connecté au téléviseur, par exemple sur une sortie de celle-ci ou directement intégré dans le téléviseur.

Dans un premier mode de réalisation, le module de réception 14 reçoit, en provenance du premier dispositif de diffusion 10 , les données chiffrées cw(CT) au moyen de mots de contrôle ainsi que les mots de contrôle cw eux-mêmes. Il reçoit également les messages d'autorisation EMM provenant d'un des deuxièmes centres 11 de diffusion. Le module de réception 14 transmet les mots de contrôle cw au module de gestion des droits. Cette transmission peut être effectuée au moyen d'ondes infrarouge ou radio par exemple. Ce module de gestion des droits vérifie qu'il a bien acquis les droits correspondants à l'événement choisi. Si tel est le cas, les messages de contrôle ECM sont traités dans le module de sécurité de façon à en extraire les mots de contrôle cw. Ceux-ci sont ensuite transmis, à une fréquence adéquate correspondant à la fréquence utilisée pour le chiffrement des données, au module de réception 14 qui les utilise alors pour déchiffrer les données et rendre ainsi visible l'événement.

Dans un deuxième mode de réalisation, illustré schématiquement par la figure 2, le flux contenant les données chiffrées, les messages de contrôle et les messages d'autorisation sont reçus par le dispositif de gestion des droits 15. Ces flux sont traités comme précédemment et les données déchiffrées sont transmises en clair au dispositif de réception.

Ce système permet de réaliser un décodeur aisément transportable et qui peut être utilisé sur n'importe quel téléviseur. Dans le cas où le module de réception des données 14 est intégré au téléviseur, il suffit de disposer du module de gestion 15 pour avoir accès à un événement. De cette façon, les contraintes pour les utilisateurs sont supprimées. En outre, le fait d'utiliser des deuxièmes centres de diffusion pour les messages d'autorisation, distincts du premier centre de diffusion des données augmente le choix offert à l'utilisateur et facilite l'emploi de systèmes à accès conditionnel.

**Revendications**

1. Système de déchiffrement de données à accès conditionnel, caractérisé en ce qu'il comporte

- un premier centre de diffusion (10) agencé pour diffuser des données chiffrées par des mots de contrôle (cw), ces mots de contrôle étant transmis par des messages de contrôle (ECM) par ce premier centre de diffusion,
- au moins un deuxième centre de diffusion (11) agencé pour diffuser des messages d'autorisation (EMM) relatifs aux droits d'accès aux données chiffrées et pour gérer ces droits d'accès,
- un dispositif d'exploitation (12) destiné à rendre utilisables lesdites données chiffrées, et
- un décodeur (13) agencé pour déchiffrer au moins une partie des données chiffrées, interposé entre le premier centre de diffusion (10) et le dispositif d'exploitation (12),

en ce que le décodeur (13) est formé d'un module de réception (14) des données chiffrées et d'un module de gestion (15) des droits d'accès à ces données, le module de réception (14) étant connecté au dispositif d'exploitation (12) et le module de gestion (15) étant agencé pour communiquer avec le module de réception,

en ce que le module de gestion (15) comporte un module de sécurité (16) agencé pour vérifier le contenu des messages d'autorisation (EMM) et pour permettre ou empêcher le déchiffrement des mots de contrôle (cw) en fonction du contenu des messages d'autorisation,

et en ce que le module de réception reçoit les données chiffrées provenant du premier centre de diffusion (10) ainsi que les mots de contrôle (cw), et le module de gestion reçoit les messages d'autorisation (EMM) du deuxième centre (11) de diffusion.

2. Système de déchiffrement de données selon la revendication 1, caractérisé en ce que la communication entre le module de réception (14) et le module de gestion (15) est une communication par ondes.

3. Système de déchiffrement de données selon la revendication 1, caractérisé en ce que le module de gestion (15) des droits est un téléphone portable.

4. Système de déchiffrement de données selon la revendication 1, comportant au moins deux deuxièmes centres de diffusion (11), caractérisé en ce que le module de sécurité (16) du module de gestion (15) comporte des moyens de lecture de messages d'autorisation (EMM) provenant de deuxièmes centres de diffusion (11) distincts.

5. Système de déchiffrement de données selon la revendication 1, caractérisé en ce que le module de réception (14) reçoit les données chiffrées directement depuis le premier dispositif de diffusion (10) et en ce que le module de gestion (15) reçoit uniquement les messages d'autorisation (EMM).

6. Système de déchiffrement de données selon la revendication 1, caractérisé en ce que le module de gestion (15) reçoit les données chiffrées, les messages de contrôle (ECM) et les messages d'autorisation (EMM) et en ce qu'il transmet les données déchiffrées au module de réception (14).

7. Système de déchiffrement de données selon la revendication 1, caractérisé en ce que le module de réception (14) est intégré dans le dispositif d'exploitation (12).

8. Système de déchiffrement de données selon la revendication 1, caractérisé en ce que le module de réception (14) est amovible par rapport au dispositif d'exploitation.

## ABREGE

La présente invention concerne un système de déchiffrement de données à accès conditionnel, en particulier utilisé dans le domaine de la télévision numérique à péage.

Ce système comporte un premier centre de diffusion (10) agencé pour diffuser des données chiffrées par des mots de contrôle (cw), au moins un deuxième centre de diffusion (11) agencé pour diffuser des messages d'autorisation (EMM) relatifs aux droits d'accès aux données chiffrées et pour gérer ces droits d'accès, un dispositif d'exploitation (12) destiné à rendre utilisables lesdites données chiffrées, et un décodeur (13) agencé pour déchiffrer au moins une partie des données chiffrées Ce décodeur est interposé entre le premier centre de diffusion (10) et le dispositif d'exploitation (12). Ce décodeur (13) est formé d'un module de réception (14) des données chiffrées et d'un module de gestion (15) des droits d'accès à ces données. Le module de réception (14) est connecté ou intégré au dispositif d'exploitation (12) et le module de gestion (15) est agencé pour communiquer avec le module de réception. Le module de gestion (15) comporte un module de sécurité (16) agencé pour vérifier le contenu des messages d'autorisation (EMM) et pour permettre ou empêcher le déchiffrement des mots de contrôle (cw) en fonction du contenu des messages d'autorisation. Le module de réception reçoit les données chiffrées provenant du premier centre de diffusion (10) ainsi que les mots de contrôle (cw), et le module de gestion reçoit les messages d'autorisation (EMM) du deuxième centre (11) de diffusion.

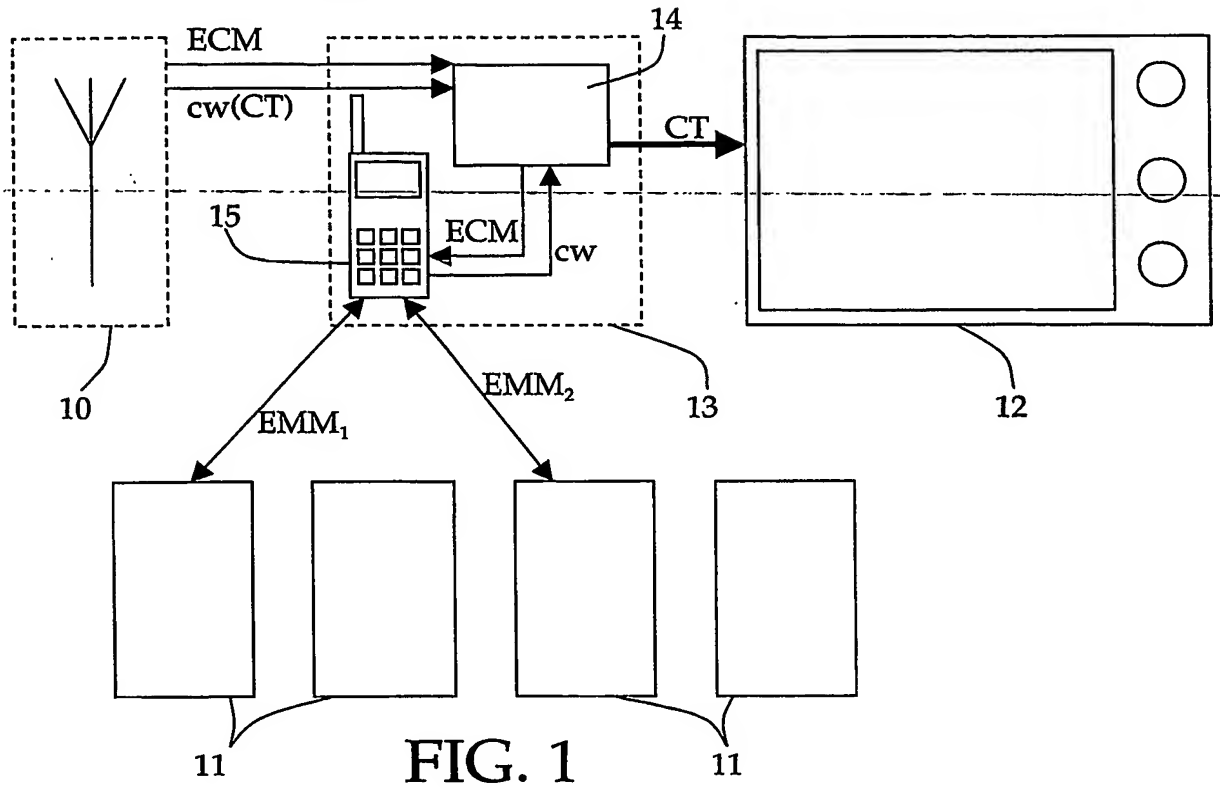


FIG. 1

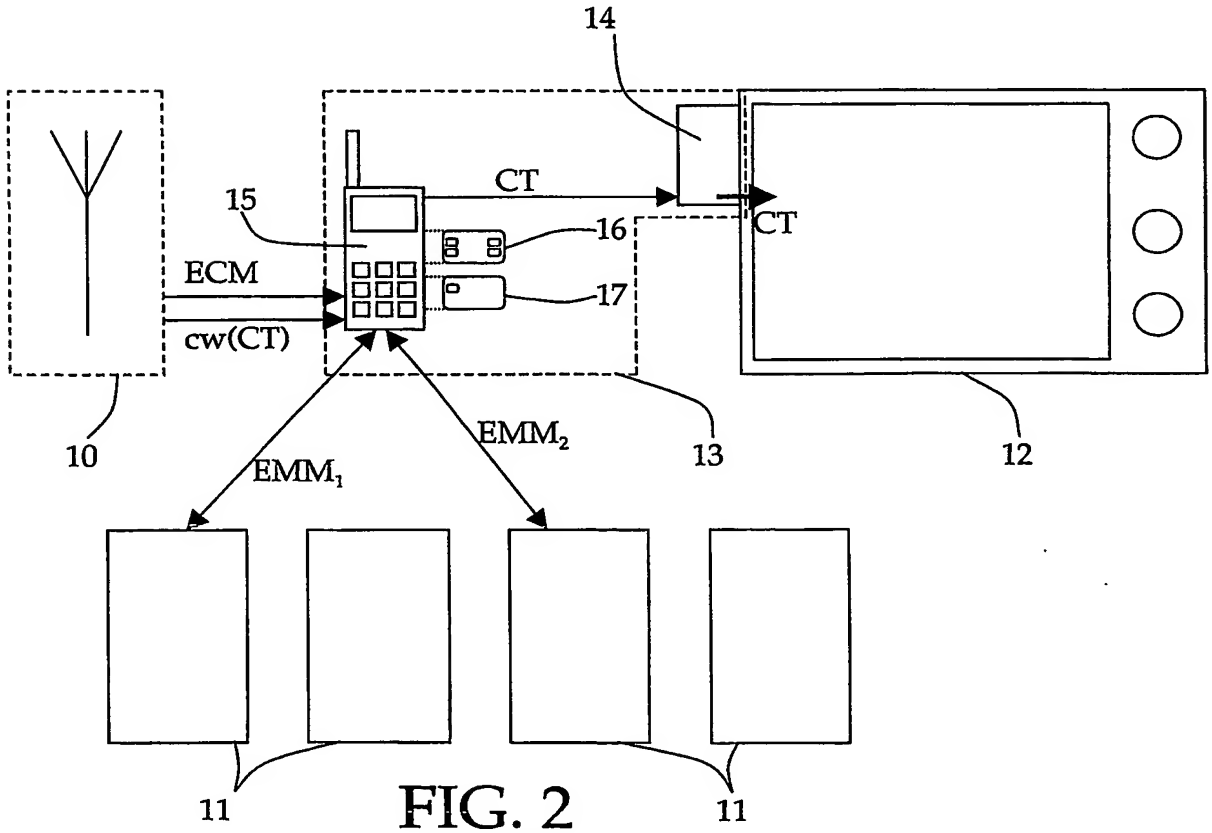


FIG. 2

# This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

## BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☑ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

**IMAGES ARE BEST AVAILABLE COPY.**
**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**